REMARKS

In response to the Office Action mailed October 20, 2006, Applicant respectfully requests reconsideration. Claims 1-11 were previously pending in this application. Claims 1-11 have been amended. New claims 12-16 have been added. As a result, claims 1-16 are pending for examination with claims 1, 9, and 14 being independent. No new matter has been added.

I. Objections to the Specification

The Office Action objected to the specification stating that the specification should have a section titled "Drawing". Applicant has added a section entitled "Brief Description of the Drawings."

Accordingly, withdrawal of this objection is respectfully requested.

II. Rejections under 35 U.S.C. §112

The Office Action rejected claims 1-11 under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention.

Applicants have amended the claims as shown above to correct the indefinite language. Accordingly, withdrawal of this rejection is respectfully requested.

III. Rejections Under 35 U.S.C. §102

The Office Action rejected claims 1, 7 and 9 under 35 U.S.C. §102 as being anticipated by U.S. Patent No. 5,974,151 ("Slavin"). Applicants respectfully disagree.

A. Claims 1-8 and 13

Independent claim 1, as amended, is directed to a method for masking digital data processed by a circuit executing an encryption algorithm. The method comprises: calculating a plurality of factorizations of at least two input data based on a variable factorization base, the variable factorization base being comprised of elements prime to one another; performing elementary operations on the plurality of factorizations to calculate a result factorization; and combining the result factorization based on the variable factorization base to obtain a result.

Slavin does not teach or suggest all the limitations of claim 1. Specifically, Slavin does

not teach calculating a plurality of factorizations of at least two input data based on a variable factorization base, the variable factorization base being comprised of elements prime to one another. Nowhere does Slavin disclose factorizing input data, and thus certainly does not disclose factorizing input data based on a variable factorization base comprised of elements prime to one another.

Therefore, claim 1 distinguishes patentably over the art of record.

Claims 2-8, and 13 depend from claim 1 and are allowable for at least the same reasons.

Accordingly, withdrawal of the rejection is respectfully requested.

B. Claims 9-12

Independent claim 9, as amended, is directed to a circuit comprising a circuit to select a variable factorization base, the variable factorization base being comprised of elements prime to one another; at least one circuit to calculate factorizations of input data based on the variable factorization base; a circuit to perform elementary operations on the factorizations to calculate a result factorization; a circuit to combine the result factorization based on the variable factorization base to obtain a result.

For reasons that should be appreciated from the above discussion, Slavin does not teach or suggest all the limitations of claim 9. Specifically, Slavin does not teach or suggest "a circuit to select a variable factorization base, the variable factorization base being comprised of elements prime to one another" and "at least one circuit to calculate factorizations of input data based on the variable factorization base." Nowhere does Slavin disclose calculating factorizations of input data, and thus certainly does not disclose calculating factorizations of input data based on a variable factorization base comprised of elements prime to one another.

Therefore, claim 9 distinguishes patentably over the art of record.

Claims 10-12 depend from claim 9 and are allowable for at least the same reasons.

Accordingly, withdrawal of the rejection is respectfully requested.

IV. New claims 14-16

New claims 14-16, have been added to further define Applicants' contribution to the art. Independent claim 14 recites, *inter alia*, "means for selecting a variable factorization base, the variable factorization base being comprised of elements prime to one another" and "at least one

circuit to calculate factorizations of input data based on the variable factorization base." Slaving does not teach or suggest at least this limitation. Claims 15-16 depend from claim 14. Thus, these claims also distinguish over Slavin for at least the reasons discussed above.

CONCLUSION

In view of the foregoing amendments and remarks, this application should now be in condition for allowance. A notice to this effect is respectfully requested. If the Examiner believes, after this amendment, that the application is not in condition for allowance, the Examiner is requested to call the Applicants' representative at the telephone number indicated below to discuss any outstanding issues relating to the allowability of the application.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicants hereby request any necessary extension of time. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 23/2825.

Dated: February 20, 2007

Respectfully submitted,

By: _____

James H. Morris
Registration No.: 34,681
WOLF, GREENFIELD & SACKS, P.C.
Federal Reserve Plaza
600 Atlantic Avenue
Boston, Massachusetts 02210-2206
(617) 646-8000